



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1470
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/002,694 | 10/31/2001 | Richard L. Schertz | 10017330-1 | 4657 |

7590 10/06/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

SON, LINH L D

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2135

DATE MAILED: 10/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/002,694

Applicant(s)

SCHERTZ ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This Office Action is responding to the amendment filed on 06/27/05.
2. Claims 1-23 are pending. None of the claims has been amended.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crosbie et al, US Publication No. 2002/0083343A1, hereinafter "Crosbie", in view of Sherlock et al, US/2002/0093527, hereinafter "Sherlock".
5. As per claims 1, 9, and 16, Crosbie teaches "A method of presenting data related to an intrusion event on a computer system (Para 0003), comprising: capturing data related to the intrusion event (Para 0007); decoding the captured data from a predetermined format (IDDS Kernel Drive, Fig. 3) to a predetermined format decipherable by humans (ASCII format, Para 0168-171). Further, Crosbie discloses that the decoded data in turn comprises of intrusion event data in (Para 162). However, Crosbie does not specifically disclose "the decoded data in turn comprises data summary, and detailed data; and presenting the decoded data to a user in an

Art Unit: 2135

organized manner. Nevertheless, Sherlock discloses the "User Interface for a Security Policy system and Method" invention, which teaches a method of capturing the network data information and get processed by the monitor policy engine to output the user in an organized way (Para 0283, Table M, 0284, Figure 9, and Figure 22-32).

Therefore, it would have been obvious for one having ordinary skill in the art at the time of the invention was made to modify Crosbie's invention to include the report feature of Sherlock to provide a presentable and understandable data captured.

6. As per claim 2, Crosbie and Sherlock teach "The method, as set forth in claim 1, wherein capturing data comprises capturing network data packets of the intrusion event" in (Para 0162).

7. As per claims 3, 11, and 18, Crosbie and Sherlock teach "The method, as set forth in claims 1, 9, and 16, wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format" in (Para 162, and 169).

8. As per claims 4, 12, and 19, Crosbie and Sherlock teach "The method, as set forth in claims 1, 9, and 16, wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in

hexadecimal format” in (Sherlock, Para 0045, and 0417-418).

9. As per claims 5, 13, and 20, Crosbie and Sherlock teach “The method, as set forth in claims 1, 9, and 16, wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format” (Sherlock, Para 045, and 0417-418).

10. As per claims 6 and 21, Crosbie and Sherlock teach “The method, as set forth in claims 1 and 16, wherein presenting the decoded data comprises displaying the decoded data on a computer screen” in (Sherlock, Para 0491-0507, Fig 22-32).

11. As per claims 7, 14, and 22, Crosbie and Sherlock teach “The method, as set forth in claims 1, 9, and 16, wherein presenting the decoded data comprises graphically displaying the decoded data according to a predetermined report organization and format” in (Sherlock, Para 0491-0507, Fig 22-32).

12. As per claims 8, 15, and 23, Crosbie and Sherlock teach “The method, as set forth in claims 1 and 16, wherein presenting the decoded data comprises generating a report having the decoded data” in (Sherlock, Para 0491-0507, Fig 22-32).

Art Unit: 2135

13. As per claims 10 and 17, Crosbie and Sherlock teach "The method, as set forth in claims 9 and 16, wherein capturing data comprises capturing network data packets of the intrusion event in response to detecting the presence of a predetermined signature in the network data packet" in (Sherlock, Table 0, MD5 Hash of policy file).

Response to Arguments

14. Applicant's argument, see Amendment, filed 06/27/05, with respect to the rejection(s) of claim(s) 1-23 under 35 U.S.C. 102(e) rejection have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Crosbie and Sherlock. See the rejection above.

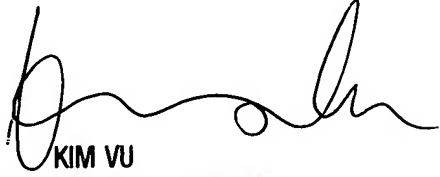
15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100